*The FBI's Counterintelligence Division produces the **FBI Monthly Counterintelligence Bulletin** to keep federal, state, local, and private sector partners informed about counterintelligence threats and issues.*

The bulletin's contents are unclassified and available via open sources. Recipients are encouraged to share the bulletin with their partners throughout the U.S. and international law enforcement and intelligence communities, as well as the private sector, as they deem appropriate.

November 2019

Chinese National Pleads Guilty to Committing Theft of Trade Secrets

Chinese national and U.S. legal permanent resident Hongjin Tan pleaded guilty on November 12 in U.S. District Court for the Northern District of Oklahoma to theft of a trade secret, unauthorized transmission of a trade secret, and unauthorized possession of a trade secret. In his plea agreement, Tan admitted he stole information regarding the manufacture of a product estimated to be worth more than $1 billion from his former employer, a petroleum company based in Oklahoma, for his own financial benefit. His sentencing is scheduled for February 2020, and he faces 18 to 24 months in prison. Read about the plea.

Ohio Man Sentenced to Prison for Illegally Exporting Goods to Iran

Iranian-born naturalized U.S. citizen Behrooz Behroozian was sentenced on October 24 in U.S. District Court for the Southern District of Ohio to 20 months in prison for illegally sending dual-use, export-controlled goods to Iran to advance its military and economic capabilities. In his plea agreement, Behroozian admitted he exported gas and oil pipeline parts with both commercial and military applications to Iran for more than a decade, using an intermediary firm and a front company to conceal his violation of export controls and U.S. embargo and trade sanctions. Read about the sentencing.

New York Company and Its Senior Management Charged with Fraud, Money Laundering, and Illegal Importation of Equipment Manufactured in China

A criminal complaint unsealed on November 7 in U.S. District Court for the Eastern District of New York charged Aventura Technologies and seven of its current and former employees for their alleged roles in a scheme to sell Chinese-made equipment with known cybersecurity vulnerabilities to U.S. government, military, and private customers while claiming the products were manufactured in the United States. According to court documents, Aventura—a surveillance and security equipment company based in New York—made nearly $88 million, including more than $20 million in government contracts, by importing products primarily from China and reselling them as American-made. By doing so, the company allegedly exposed its customers to serious cybersecurity risks and created a channel foreign adversaries could have used to access some of the U.S. government's most sensitive facilities. Six of the defendants were arrested, and the seventh turned himself in. If convicted, they face up to 20 years in prison for each count. Read about the charges.

Iranian Businessman Sentenced to 46 Months in Prison for Violating U.S. Sanctions by Exporting Carbon Fiber from the United States to Iran

Iranian national Behzad Pourghannad was sentenced on November 13 in U.S. District Court for the Southern District of New York to 46 months in prison for his role in a conspiracy to export tons of carbon fiber from the United States to Iran via third countries, in violation of U.S. sanctions. Carbon fiber is strictly controlled and has a variety of aerospace and defense applications, including in missiles and centrifuges used to enrich uranium. Pourghannad was arrested in Germany in 2017 and pleaded guilty in August 2019 after his extradition to the United States. His co-conspirators, Iranian nationals Ali Reza Shokri and Farzin Faridmanesh, remain at large and, if convicted, face up to 20 years in prison for each of three counts. Read about the sentencing.

U.S. Navy Officer, His Wife, and Two Chinese Nationals Charged with Conspiring to Smuggle Military-Style Inflatable Boats and Outboard Motors to China

A six-count indictment returned on October 31 in the Middle District of Florida charged four individuals—including U.S. Navy Lieutenant Fan Yang and his wife, Yang Yang—for their alleged roles in a conspiracy to unlawfully smuggle military-style inflatable boats and engines to China, in violation of export laws. The indictment also includes charges of conspiring to violate firearms law, making a false statement to a firearms dealer, making false official statements, and false export information. All four defendants were arrested on October 17. If convicted, they face maximum sentences ranging from five to 10 years for each of the counts. Read about the charges.

U.S. Government Agencies Issue Joint Statement on Safeguarding Election Security

The FBI joined the Office of the Director of National Intelligence, National Security Agency, and U.S. Departments of Defense, Justice, and Homeland Security to issue a joint statement on November 5 regarding work to combat the threat posed by foreign influence operations targeting U.S. elections. Citing unprecedented levels of coordination across the federal, state, local, and territorial levels, the statement emphasized the government's commitment to sharing information, services, and support to defend against foreign adversaries' efforts to undermine American democratic institutions, influence public sentiment, and affect U.S. policies. The statement also encouraged the public to seek out trusted sources for election information and report suspicious activity. Read the joint statement.

FBI Director Discusses Counterintelligence Threats During Senate Hearing

FBI Director Christopher Wray discussed the current and emerging threat environment on November 5 during an open hearing before the U.S. Senate Committee on Homeland Security and Governmental Affairs. During the hearing, Director Wray discussed counterintelligence threats ranging from election interference to economic espionage and emphasized the importance of engagement and collaboration with academic institutions and the private sector. Watch a video of the hearing or read Director Wray's statement for the record.

MEDIA HIGHLIGHT

The following information has been prepared by outlets outside the U.S. government and has not been corroborated by the FBI or its partners. It is presented here for your situational awareness.

Foreign Policy Ties China's Central Asia Partnerships to Data Collection and Surveillance

In a November 15 article, *Foreign Policy,* an American news publication, reported on the expansion of China's "advanced surveillance regime" via its Digital Silk Road initiative, which aims to construct a China-centric digital infrastructure by establishing smart cities across Central Asia. Citing Chinese companies' deals to supply telecommunications infrastructure and equipment—including video surveillance systems and facial recognition software—to Uzbekistan, Kyrgyzstan, and Tajikistan, the article highlighted concerns the partnerships could help Central Asian nations monitor their own populations. The report also raised the prospect that partnerships throughout the region could give China access to large swaths of personal data while helping it track the cross-border movement of the Uighurs and other ethnic minorities. Read the *Foreign Policy* article.

This Monthly Counterintelligence Bulletin is prepared by the FBI's Counterintelligence Division.
To report a counterintelligence matter, contact your local FBI office.